REMARKS

Claims 1-30 were originally filed in the present application. Claims 16-26 were previously withdrawn. Claims 1-15 and 27-30 were rejected in a Final Office Action dated June 13, 2008. An Amendment After Final was filed on September 15, 2008. The Amendment After Final included amendments to claims 27, 28 and 30. An Advisory Action was mailed on October 1, 2008 indicating that the Amendment After Final failed to place the application in condition for allowance. Applicant appealed the rejection of claims 1-15 and 27-30 in the Final Action in an Appeal Brief filed on January 13, 2009. The Office Action dated April 29, 2009 indicates that in view of the Appeal Brief, prosecution has been reopened. Accordingly, Applicant submits that claims 1-15 and 27-30 are pending in the present application. Claims 1-15 and 28-29 stand rejected in the present application. Claims 27 and 28 have been amended by way of this amendment. Claims 1-15 and 28-30 remain pending.

Claim 28 has been objected to as failing to provide sufficient antecedent basis for the limitation "the encrypted encryption keys." Claim 28 has been amended to so that appropriate antecedent basis has been provided for the limitations in the claim. Accordingly, Applicant respectfully requests the withdrawal of the objection to claim 28.

Claim 27 has also been amended to provide proper antecedent basis.

Claim 1 stands rejected under 35 USC §102(b) as being anticipated by Eisele (US Patent No. 5,159,182). Claims 2-15 and 28-29 stand rejected under 35 USC §102(b) as being anticipated by or, in the alternative, under 35 USC §103(a) as being obvious over Eisele.

Turning first to the rejection of claims 1-15 and 28-29 as being anticipated by Eisele, "A claim is anticipated if each and every element as set forth in the claim is found, either expressly or inherently described, in a single, prior art reference." Verdegaal Bros. v. Union Oil Co., of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Applicant respectfully traverses the rejection of claims 1-5 and 28-29 as being anticipated by Eisele.

Independent claim 1 and claims 2-15 dependent thereon recite a removable information storage device suitable for use with a host. The removable information

storage device includes *inter alia* a non-volatile memory configured to store a master encryption key and a non-volatile magnetic memory configured to store encryption keys which have been encrypted using the master encryption key and to store data which has been encrypted using the encryption keys.

Eisele generally discloses insertable devices, such as for example diskettes, for use with electronic data processing (EDP) equipment. Referring to FIG. 2, a first disclosed diskette 7 includes a diskette processor 2 coupled to a magnetic interface 6 via a diskette driver 4. The diskette processor 2 may be connected to additional memory 9 within the diskette. The diskette processor 2 communicates with EDP-equipment, such as for example a central computer, via the magnetic interface 6. (See col. 4, lines 1-6 and lines 14-17). Referring to FIG. 3, a second disclosed diskette 7 includes a magnetic disk 15 that operates as an intermediate storage facility between the diskette processor 2 and EDP-equipment or central computer. More specifically, data supplied by the diskette processor 2 is initially stored on the magnetic disk 15. The data stored on the magnetic disk 15 is read by the EDP-equipment or central computer. The diskette processor may be connected to additional memory 9. (See col. 4, lines 18-28). The diskette processor 2 disclosed in Eisele may be used to encrypt and decrypt data. (See col. 5, lines 12-16). The memory units in a diskette are first loaded with one or more cryptographic algorithms and/or secret codes etc. in such a way that they cannot be reproduced (see col. 5, lines 20-24). Plaintext is transmitted from an external device to the diskette processor 2 via the diskette interface. The diskette processor 2 encrypts the received plaintext and sends the encrypted version of the plaintext back to the external device via the diskette interface. (see col. 5, lines 12-19).

While Eisele discloses loading cryptographic algorithms into the diskette memory in a way that they cannot be reproduced and the use of such cryptographic algorithms to encrypt data received at a diskette, Eisele does not disclose the use of *a non-volatile memory configured to store a master encryption key and the use of a non-volatile magnetic memory configured to store encryption keys which have been encrypted using the master encryption key* as recited by claims 1-15. There is no teaching in Eisele directed to the use of a master encryption key to encrypt encryption keys. Furthermore, Eisele does not teach the use of two different memories to store encryption keys, i.e. a non-volatile memory to store the master encryption key and a non-volatile magnetic memory to store the encrypted encryption keys as recited by claims 1-15. Since Eisele

fails to disclose each and every element recited by claims 1-15, Applicant respectfully requests the withdrawal of the rejection of such claims as being anticipated by Eisele.

Independent claim 28 and claims 29 dependent thereon recite a method of decrypting encryption keys in an information storage device. The method includes *inter alia* reading encrypted encryption keys from a magnetic random access memory, reading a master encryption key from a first non-volatile memory and decrypting each one of the encryption keys using the master encryption key.

While Eisele discloses the use of a diskette processor 2 to encrypt and decrypt data, Eisele does not disclose *reading encrypted encryption keys from a magnetic random access memory, reading a master encryption key from a first non-volatile memory and decrypting each one of the encryption keys using the master encryption key*. There is no teaching in Eisele directed to the use of a master encryption key to decrypt encrypted encryption keys. Furthermore, Eisele does not disclose the use of two different memories, i.e. reading encrypted encryption keys from a magnetic random access memory and reading a master encryption key from a first non-volatile memory as recited by claims 28-29. Since Eisele fails to disclose each and every element recited by claims 28-29, Applicant respectfully requests the withdrawal of the rejection of such claims as being anticipated by Eisele.

Turning now to the rejection of claims 2-15 and 28-29 under 35 USC §103(a) as being unpatentable over Eisele, the test for determining if a claim is rendered obvious by one or more references for purposes of a rejection under 35 U.S.C. § 103 is set forth in KSR International Co. v. Teleflex Inc., 550 U.S._, 82 USPQ2d 1385 (2007):

> "Under §103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented." Quoting Graham v. John Deere Co. of Kansas City, 383 U.S. 1 (1966).

As set forth in MPEP 2143.03, to ascertain the differences between the prior art and the claims at issue, "[a]ll claim limitations must be considered" because "all words in a claim must be considered in judging the patentability of that claim against the prior art."

In re Wilson, 424 F.2d 1382, 1385. According to the Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in view of KSR International Co. v. Teleflex Inc., Federal Register, Vol. 72, No. 195, 57526, 57529 (October 10, 2007), once the Graham factual inquiries are resolved, there must be a determination of whether the claimed invention would have been obvious to one of ordinary skill in the art based on any one of the following proper rationales:

> (A) Combining prior art elements according to known methods to yield predictable results; (B) Simple substitution of one known element for another to obtain predictable results; (C) Use of known technique to improve similar devices (methods, or products) in the same way; (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (E) "Obvious to try"— choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; (F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention. KSR International Co. v. Teleflex Inc., 550 U.S._, 82 USPQ2d 1385 (2007).

Furthermore, as set forth in KSR International Co. v. Teleflex Inc., quoting from In re Kahn, 441 F.3d 977, 988 (CA Fed. 2006), "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasonings with some rational underpinning to support the legal conclusion of obviousness."

Therefore, if the above-identified criteria and rationales are not met, then the cited reference(s) fails to render obvious the claimed invention and, thus, the claimed invention is distinguishable over the cited reference(s).

Claims 2-15 dependent from independent claim 1 and therefore include the elements of independent claim 1. Eisele does not disclose the use of _a non-volatile memory configured to store a master encryption key and the use of a non-volatile magnetic memory configured to store encryption keys which have been encrypted using the master encryption key_ as recited by claims 2-15. There is no teaching in Eisele directed to the use of a master encryption key to encrypt encryption keys. Furthermore, Eisele does not teach the use of two different memories to store encryption keys, i.e. a

non-volatile memory to store the master encryption key and a non-volatile magnetic memory to store the encrypted encryption keys as recited by claims 2-15. Accordingly, Applicant respectfully requests the withdrawal of the rejection claims 2-15 as being unpatentable under 35 USC §103(a).

With respect to the rejection of independent claim 28 and claim 29 dependent thereon, Eisele fails to disclose *reading encrypted encryption keys from a magnetic random access memory, reading a master encryption key from a first non-volatile memory and decrypting each one of the encryption keys using the master encryption key* as recited by claims 28-29. There is no teaching in Eisele directed to the use of a master encryption key to decrypt encrypted encryption keys. Furthermore, Eisele does not disclose the use of two different memories, i.e. reading encrypted encryption keys from a magnetic random access memory and reading a master encryption key from a first non-volatile memory as recited by claims 28-29. Accordingly, Applicant respectfully requests the withdrawal of the rejection claims 28-29 as being unpatentable under 35 USC §103(a).

For the foregoing reasons, reconsideration and withdrawal of the rejection of the claims at issue and allowance thereof are respectfully requested.

Respectfully submitted,

By: _Manisha Chakrabarti_
Manisha Chakrabarti
Attorney Reg. No. 41,665

Manisha Chakrabarti
Attorney at Law
3108 South Route 59, Suite 124-282
Naperville, Illinois 60564
Date: July 29, 2009   Telephone: (630) 355-3376